

**What Is Claimed Is:**

1           1.       A method for establishing a cryptographic key for use between a  
2 first node and a second node using a super node, wherein the first node and the  
3 second node are energy-limited and the super node has abundant energy, the  
4 method comprising:  
5           sending a first message from the first node to the super node, wherein the  
6 first message includes a first partial key value encrypted using a public key  
7 belonging to the super node, whereby encrypting with the public key requires less  
8 energy than decrypting with a private key corresponding to the public key;  
9           recovering the first partial key value at the super node by decrypting using  
10 the private key;  
11           securely communicating the first partial key value to the second node; and  
12           establishing the cryptographic key at the second node using the first partial  
13 key value and a second partial key value created by the second node;  
14           whereby energy usage is shifted to the super node by performing private  
15 key decryption at the super node.

1           2.       The method of claim 1, further comprising sending a second  
2 message from the first node to the second node, wherein the second message  
3 includes a first message authentication code.

1           3.       The method of claim 2, further comprising authenticating the first  
2 partial key value at the second node using the first message authentication code.

1           4.       The method of claim 1, further comprising:





1           13.     The method of claim 12, wherein the certificate includes validation  
2 information for a plurality of symmetric keys and wherein a new first node  
3 symmetric key is selected periodically from the plurality of symmetric keys.

1           14.     The method of claim 11, wherein the first node symmetric key is  
2 saved at the super node so that a subsequent key establishment can use symmetric  
3 key encryption for encrypting the second partial key value.

1           15.     The method of claim 4, wherein establishing the cryptographic key  
2 at the first node involves creating a hash of the first partial key value and the  
3 second partial key value.

1           16.     The method of claim 4, wherein establishing the cryptographic key  
2 at the second node involves creating a hash of the first partial key value and the  
3 second partial key value.

1           17.     The method of claim 4, further comprising establishing trust of the  
2 super node at the first node by validating a certificate provided by a recognized  
3 certificate authority and presented to the first node by the super node.

1           18.     The method of claim 4, further comprising establishing trust of the  
2 super node at the second node by validating a certificate provided by a recognized  
3 certificate authority and presented to the second node by the super node.

1           19.     A computer-readable storage medium storing instructions that  
2 when executed by a computer cause the computer to perform a method for  
3 establishing a cryptographic key for use between a first node and a second node

4 using a super node, wherein the first node and the second node are energy-limited  
5 and the super node has abundant energy, the method comprising:  
6 sending a first message from the first node to the super node, wherein the  
7 first message includes a first partial key value encrypted using a public key  
8 belonging to the super node, whereby encrypting with the public key requires less  
9 energy than decrypting with a private key corresponding to the public key;  
10 recovering the first partial key value at the super node by decrypting using  
11 the private key;  
12 securely communicating the first partial key value to the second node; and  
13 establishing the cryptographic key at the second node using the first partial  
14 key value and a second partial key value created by the second node;  
15 whereby energy usage is shifted to the super node by performing private  
16 key decryption at the super node.

1 20. The computer-readable storage medium of claim 19, the method  
2 further comprising sending a second message from the first node to the second  
3 node, wherein the second message includes a first message authentication code.

1 21. The computer-readable storage medium of claim 20, the method  
2 further comprising authenticating the first partial key value at the second node  
3 using the first message authentication code.

1 22. The computer-readable storage medium of claim 19, the method  
2 further comprising:  
3 sending a third message from the second node to the super node, wherein  
4 the third message includes the second partial key value encrypted using the public  
5 key belonging to the super node;

6 recovering the second partial key value at the super node by decrypting  
 7 using the private key;  
 8 securely communicating the second partial key value to the first node; and  
 9 establishing the cryptographic key at the first node using the first partial  
 10 key value and the second partial key value.

1 23. The computer-readable storage medium of claim 22, the method  
 2 further comprising sending a fourth message from the second node to the first  
 3 node, wherein the fourth message includes a second message authentication code.

1 24. The computer-readable storage medium of claim 23, the method  
 2 further comprising authenticating the second partial key value at the first node  
 3 using the second message authentication code.

1 25. The computer-readable storage medium of claim 22, wherein  
 2 securely communicating the first partial key value to the second node includes:  
 3 encrypting the first partial key value at the super node using a second node  
 4 symmetric key creating a first encrypted partial key value, wherein the second  
 5 node symmetric key is received in the third message;  
 6 transmitting the first encrypted partial key value to the second node; and  
 7 decrypting the first encrypted partial key value at the second node to  
 8 recover the first partial key value.

1 26. The computer-readable storage medium of claim 25, wherein the  
 2 second node symmetric key is validated using a certificate provided by a  
 3 recognized certificate authority and wherein the certificate is included in the third  
 4 message.

1           27.     The computer-readable storage medium of claim 26, wherein the  
2     certificate includes validation information for a plurality of symmetric keys and  
3     wherein a new second node symmetric key is selected periodically from the  
4     plurality of symmetric keys.

1           28.     The computer-readable storage medium of claim 25, wherein the  
2     second node symmetric key is saved at the super node so that a subsequent key  
3     establishment can use symmetric key encryption for encrypting the first partial key  
4     value.

1           29.     The computer-readable storage medium of claim 22, wherein  
2     securely communicating the second partial key value to the first node includes:  
3             encrypting the second partial key value at the super node using a first node  
4     symmetric key creating a second encrypted partial key value, wherein the first  
5     node symmetric key is received in the first message and wherein the first node  
6     symmetric key is encrypted using the public key belonging to the super node;  
7             transmitting the second encrypted partial key value to the first node; and  
8             decrypting the second encrypted partial key value at the first node to  
9     recover the second partial key value.

1           30.     The computer-readable storage medium of claim 29, wherein the  
2     first node symmetric key is validated using a certificate provided by a recognized  
3     certificate authority and wherein the certificate is included in the first message.

1           31.     The computer-readable storage medium of claim 30, wherein the  
2     certificate includes validation information for a plurality of symmetric keys and

3 wherein a new first node symmetric key is selected periodically from the plurality  
4 of symmetric keys.

1 32. The computer-readable storage medium of claim 29, wherein the  
2 first node symmetric key is saved at the super node so that a subsequent key  
3 establishment can use symmetric key encryption for encrypting the second partial  
4 key value.

1 33. The computer-readable storage medium of claim 22, wherein  
2 establishing the cryptographic key at the first node involves creating a hash of the  
3 first partial key value and the second partial key value.

1 34. The computer-readable storage medium of claim 22, wherein  
2 establishing the cryptographic key at the second node involves creating a hash of  
3 the first partial key value and the second partial key value.

1 35. The computer-readable storage medium of claim 22, the method  
2 further comprising establishing trust of the super node at the first node by  
3 validating a certificate provided by a recognized certificate authority and  
4 presented to the first node by the super node.

1 36. The computer-readable storage medium of claim 22, the method  
2 further comprising establishing trust of the super node at the second node by  
3 validating a certificate provided by a recognized certificate authority and  
4 presented to the second node by the super node.





5           the second sending mechanism further configured to send a fourth  
6 message from the second node to the super node, wherein the fourth message  
7 includes the second partial key value encrypted using the public key belonging to  
8 the super node;  
9           the decrypting mechanism further configured to recover the second partial  
10 key value at the super node by decrypting using the private key;  
11           the secure communication mechanism further configured to securely  
12 communicating the second partial key value to the first node;  
13           a second authenticating mechanism configured to authenticate the second  
14 partial key value at the first node using the second message authentication code;  
15 and  
16           a second establishing mechanism configured to establish the cryptographic  
17 key at the first node using the first partial key value and the second partial key  
18 value.